UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/580,013	05/19/2006	Yukinori Suda	Q95076	7740

23373 7590 07/21/2009

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
HERRERA, DIEGO D	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
07/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/580,013	SUDA ET AL.	
	Examiner	Art Unit	
	DIEGO HERRERA	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 May 2006 and 26 July 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

Should applicant desire to obtain the benefit of foreign priority under 35 U.S.C. 119(a)-(d) prior to declaration of an interference, a certified English translation of the foreign application must be submitted in reply to this action. 37 CFR 41.154(b) and 41.202(e).

Failure to provide a certified translation may result in no benefit being accorded for the non-English application.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 5/19/2006 was filed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

Content of Specification

(a) Title of the Invention: See 37 CFR 1.72(a) and MPEP § 606. The title of the invention should be placed at the top of the first page of the specification unless the title is provided in an application data sheet. The title of the invention should be brief but technically accurate and descriptive, preferably from two to seven words may not contain more than 500 characters.

(b) Cross-References to Related Applications: See 37 CFR 1.78 and MPEP § 201.11.

(c) Statement Regarding Federally Sponsored Research and Development: See MPEP § 310.

(d) The Names Of The Parties To A Joint Research Agreement: See 37 CFR 1.71(g).

(e) Incorporation-By-Reference Of Material Submitted On a Compact Disc: The specification is required to include an incorporation-by-reference of electronic documents that are to become part of the permanent United States Patent and Trademark Office records in the file of a patent application. See 37 CFR 1.52(e) and MPEP § 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text were permitted as electronic documents on compact discs beginning on September 8, 2000.

(f) Background of the Invention: See MPEP § 608.01(c). The specification should set forth the Background of the Invention in two parts:

(1) Field of the Invention: A statement of the field of art to which the invention pertains. This statement may include a paraphrasing of the applicable U.S. patent classification definitions of the subject matter of the claimed invention. This item may also be titled "Technical Field."

(2) Description of the Related Art including information disclosed under 37 CFR 1.97 and 37 CFR 1.98: A description of the related art known to the applicant and including, if applicable, references to specific related art and problems involved in the prior art which are solved by the applicant's invention. This item may also be titled "Background Art."

(g) Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or general statement of the invention as set forth in 37 CFR 1.73. The summary is separate and distinct from the abstract and is directed toward the invention rather than the disclosure as a whole. The summary may point out the advantages of the invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). In chemical cases it should point out in general terms the utility of the invention. If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.

(h) Brief Description of the Several Views of the Drawing(s): See MPEP § 608.01(f). A reference to and brief description of the drawing(s) as set forth in 37 CFR 1.74.

(i) Detailed Description of the Invention: See MPEP § 608.01(g). A description of the preferred embodiment(s) of the invention as required in 37 CFR 1.71. The description should be as short and specific as is necessary to describe the invention adequately and accurately. Where

elements or groups of elements, compounds, and processes, which are conventional and generally widely known in the field of the invention described and their exact nature or type is not necessary for an understanding and use of the invention by a person skilled in the art, they should not be described in detail. However, where particularly complicated subject matter is involved or where the elements, compounds, or processes may not be commonly or widely known in the field, the specification should refer to another patent or readily available publication which adequately describes the subject matter.

(j) Claim or Claims: See 37 CFR 1.75 and MPEP § 608.01(m). The claim or claims must commence on separate sheet or electronic page (37 CFR 1.52(b)(3)). Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation. There may be plural indentations to further segregate subcombinations or related steps. See 37 CFR 1.75 and MPEP § 608.01(i)-(p).

(k) Abstract of the Disclosure: See MPEP § 608.01(f). A brief narrative of the disclosure as a whole in a single paragraph of 150 words or less commencing on a separate sheet following the claims. In an international application which has entered the national stage (37 CFR 1.491(b)), the applicant need not submit an abstract commencing on a separate sheet if an abstract was published with the international application under PCT Article 21. The abstract that appears on the cover page of the pamphlet published by the International Bureau (IB) of the World Intellectual Property Organization (WIPO) is the abstract that will be used by the USPTO. See MPEP § 1893.03(e).

(l) Sequence Listing. See 37 CFR 1.821-1.825 and MPEP §§ 2421-2431. The requirement for a sequence listing applies to all sequences disclosed in a given application, whether the sequences are claimed or not. See MPEP § 2421.02.

Please, submit to the above guidelines description as to what to include in a specification and in the order it is detailed, the applicant submitted a specification that is out of order and not in keeping to MPEP guidelines.

Claim Objections

Claims 1, 4-7, 18-20 are objected to because of the following informalities: they are missing a colon after the word "comprises" or "comprising". Appropriate correction is required.

Claims 6-7, 9, 11-14, 16 and 17 are objected to because of the following informalities: they are using the term "itself" as to referring to an object previously stated; however, it is not clear whether this refers to the Radio Network Controller, Virtual Private Network gateway, Corporate Private Network or Base Station. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 13-17 are drawn to a "program" *per se* as recited in the preamble and as such is non-statutory subject matter. See MPEP § 2106.IV.B.1.a. Data structures not claimed as embodied in computer readable media are descriptive material *per se* and are not statutory because they are not capable of causing functional change in the computer. See, e.g., *Warmerdam*, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure *per se* held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention, which permit the data structure's functionality to be realized. In contrast, a claimed computer readable medium encoded with a data structure defines structural and functional interrelationships between the data structure

and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory. Similarly, computer programs claimed as computer listings *per se*, i.e., the descriptions or expressions of the programs are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer, which permit the computer program's functionality to be realized. The claims 13-17 state a program allowing a computer to perform or execute functions, however, is there is no statement as to how this is done, therefore, the program has to be "embodied" on the computer and not just "allowing", this changes will have the claims not be nonstatutory. However, for the sake of compact prosecution, the above mentioned claims will be considered statutory for the time being, correction, though, is required. (See MPEP § 2106.IV.B.1.a. for guidelines)

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 8, 13, and 18 are rejected under 35 U.S.C. 102(b) as being anticipated by Watanabe et al. (US 20040192309 a1).

Regarding claim 1. A mobile communication system (fig. 9) which comprises:

a radio network controller and a radio base station connected to said radio network controller and which provides a mobile communication service to a mobile terminal connectable to said radio base station, wherein said radio base station is installed within a private network (fig. 9, ¶: 5-9, 46, Watanabe et al. teaches RAN, radio access network, which is a collective term for the radio base station and radio network controller, the RNC controls functionalities for one or more base stations. A base station and a RNC can be the same device, although common set-ups have a separate RNC located in a central office serving multiple base station, despite the fact that they don't have to be physically separated.),

a relay node installed in said private network relays mobile communication traffic transmitted on said private network between said radio network controller and said radio base station (fig. 9, ¶: 10, Watanabe et al. teaches VPN, virtual private network, as a relay node installed in said private network which in turn communicates traffic between RAN, radio access networks, and mobile terminal or devices.), and

when said mobile terminal makes or receives a call, said relay node performs reception determination processing in cooperation with bandwidth management function in said private network (fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies) and provides a communication line to said mobile terminal when permitting the reception (¶: 10, Watanabe et al. teaches access to mobile communication device through VPN to corporate intranets

over public internet, hence, providing seamless mobility between corporate intranets and access networks with mobile terminal).

Consider claim 2. The mobile communication system according to claim 1, wherein said relay node receives a bandwidth control signaling that said radio network controller transmits to said radio base station when said mobile terminal makes or receives a call to thereby start the reception determination processing (¶: 10, Watanabe et al. teaches access to mobile communication device through VPN to corporate intranets over public internet, hence, providing seamless mobility between corporate intranets and access networks with mobile terminal).

Consider claim 3. The mobile communication system according to claim 1, wherein said relay node is a VPN gateway (fig. 9; ¶: 10, Watanabe et al. teaches virtual private network, VPN, gateways as another network architecture).

Regarding claim 8. A relay node which relays mobile communication traffic between a radio base station and a radio network controller, wherein said relay node is installed in a private network in which said radio base station is installed and relays mobile communication traffic transmitted on said private network between said radio network controller and said radio base station, said relay node comprising:

means for receiving a bandwidth control signaling that said radio network controller transmits to said radio base station (fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies);

means for extracting traffic information comprises in the bandwidth control signaling;

means for performing reception determination in cooperation with a bandwidth management mechanism within said private network (abstract, fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies); and

means for transmitting the bandwidth control signaling including a result of the reception determination and bandwidth control information whose reception has been permitted (abstract, fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies).

Regarding claim 13. A relay node program allowing a computer serving as a relay node which relays mobile communication traffic between a radio base station and radio network controller to execute a function of relaying mobile communication traffic transmitted on a private network between the radio network controller and radio base station, said computer serving as a relay node and radio base station being installed within said private network, said program further allowing the computer to execute functions of:

receiving a bandwidth control signaling that said radio network controller transmits to said radio base station (fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile

terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies):

extracting traffic information comprises in the bandwidth control signaling (fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies);

performing reception determination in cooperation with a bandwidth management mechanism within said private network (fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies); and

transmitting the bandwidth control signaling including a result of the reception determination and bandwidth control information whose reception has been permitted (fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies).

Regarding claim 18. A mobile communication method (fig. 9) for use in a mobile communication system which comprises a radio network controller and a radio base station connected to said radio network controller and which provides a mobile

communication service to a mobile terminal connectable to said radio base station (fig. 9, ¶: 5-9, 46, Watanabe et al. teaches RAN, radio access network, which is a collective term for the radio base station and radio network controller, the RNC controls functionalities for one or more base stations. A base station and a RNC can be the same device, although common set-ups have a separate RNC located in a central office serving multiple base station, despite the fact that they don't have to be physically separated.), wherein said radio base station and relay node are installed within a private network comprised said the mobile communication system (fig. 9, ¶: 10, Watanabe et al. teaches VPN, virtual private network, as a relay node installed in said private network which in turn communicates traffic between RAN, radio access networks, and mobile terminal or devices.),

said relay node relays mobile communication traffic transmitted on said private network between said radio network controller and radio base station (fig. 9, ¶: 10, Watanabe et al. teaches VPN, virtual private network, as a relay node installed in said private network which in turn communicates traffic between RAN, radio access networks, and mobile terminal or devices.), and

when said mobile terminal makes or receives a call, said relay node performs reception determination processing in cooperation with bandwidth control in the private network (fig. 9, ¶: 8-10, 19-20, 35, Watanabe et al. teaches mobile terminal accessing access network to communicate and through means of authentication and selection of bearer selection based on, inter alia, available bandwidth, service classification, and network operator contract policies) and provides a communication line to said mobile terminal

when permitting the reception (¶: 10, Watanabe et al. teaches access to mobile communication device through VPN to corporate intranets over public internet, hence, providing seamless mobility between corporate intranets and access networks with mobile terminal).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 4-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Watanabe et al. (US 20040192309 a1), and in view of Forslow (US 20020069278 A1).

Regarding claim 4. A mobile communication system (fig. 9) which comprises:

a radio network controller and a radio base station connected to said radio network controller and which provides a mobile communication service to a mobile terminal connectable to said radio base station, wherein said radio base station is installed within a private network (fig. 9, ¶: 5-9, 46, Watanabe et al. teaches RAN, radio access network, which is a collective term for the radio base station and radio network controller, the RNC controls functionalities for one or more base stations. A base station and a RNC can be the same device, although common set-ups have a separate RNC located in a central office serving multiple base station, despite the fact that they don't have to be physically separated.),

a relay node installed in said private network relays mobile communication traffic transmitted on said private network between said radio network controller and said radio base station (fig. 9, ¶: 10, Watanabe et al. teaches VPN, virtual private network, as a relay node installed in said private network which in turn communicates traffic between RAN, radio access networks, and mobile terminal or devices.),

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and

secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

first and second encryption keys are used, respectively, between said radio network controller and relay node and between said radio base station and relay node to perform encrypted communication (¶: 135-139, Forslow teaches interactions between mobile client and service manager and correspondent node or gateway to a mobile station and setting security protocols between each connections to assure privacy and content protection between private network and mobile terminal through infrastructure elements), and

a pre-shared key needed to generate said second encryption key is dynamically generated by a key exchange mechanism between said radio network controller and radio base station, said generated pre-shared key being notified from said radio network controller to said relay node (¶: 135-139, Forslow teaches updating between connections of managing elements and mobile terminal and nodes or gateways take place to authenticate and authorized for session as the sessions keys are verified to take place between the private network and mobile device through nodes).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented

security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 5. A mobile communication system (fig. 9) which comprises:

a radio network controller and a radio base station connected to said radio network controller and which provides a mobile communication service to a mobile terminal connectable to said radio base station, wherein said radio base station is installed within a private network, mobile communication traffic between a relay node which is connected to said radio base station via said private network and said radio base station is transmitted on said private network (fig. 9, ¶: 5-9, 46, Watanabe et al. teaches RAN, radio access network, which is a collective term for the radio base station and radio network controller, the RNC controls functionalities for one or more base stations. A base station and a RNC can be the same device, although common set-ups have a separate RNC located in a central office serving multiple base station, despite the fact that they don't have to be physically separated.),

said relay node relays the mobile communication traffic transmitted on said private network between said radio network controller and said radio base station (fig. 9, ¶: 10, Watanabe et al. teaches VPN, virtual private network, as a relay node installed in said private network which in turn communicates traffic between RAN, radio access networks, and mobile terminal or devices.),

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

first and second encryption keys are used, respectively, between said radio network controller and relay node and between said radio base station and relay node to perform encrypted communication (¶: 135-139, Forslow teaches interactions between mobile client and service manager and correspondent node or gateway to a mobile station and setting security protocols between each connections to assure privacy and content protection between private network and mobile terminal through infrastructure elements), and

said second encryption key is dynamically generated by a key exchange mechanism between said radio network controller and said radio base station, the generated second encryption key being notified from said radio network controller to said relay node (¶: 135-139, Forslow teaches updating between connections of managing elements and mobile terminal and nodes or gateways take place to authenticate and authorized for session as the sessions keys are verified to take place between the private network and mobile device through nodes).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Consider claim 6. The mobile communication system according to claim 4, wherein said radio network controller comprises means for dynamically generating said pre-shared key by using a key exchange mechanism between itself and said radio base station, and means for notifying said relay node of said generated pre- shared key.

Consider claim 7. The mobile communication system according to claim 5, wherein said radio network controller comprises means for dynamically generating said second encryption key by using a key exchange mechanism between itself and said radio base station, and means for notifying said relay node of said generated second encryption key.

Regarding claim 9. A relay node which relays mobile communication traffic between a radio base station and a radio network controller (fig. 9), wherein said relay node is installed in a private network in which said radio base station is installed and relays mobile communication traffic transmitted on said private network between said radio

network controller and said radio base station (fig. 9, ¶: 5-9, 46, Watanabe et al. teaches RAN, radio access network, which is a collective term for the radio base station and radio network controller, the RNC controls functionalities for one or more base stations. A base station and a RNC can be the same device, although common set-ups have a separate RNC located in a central office serving multiple base station, despite the fact that they don't have to be physically separated.), and said relay node is connected to said radio base station and radio network controller and performs encrypted communication with said radio network controller by using a first encryption key and with said radio base station by using a second encryption key, said relay node comprising:

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135-139; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

means for receiving a pre-shared key for generating the second encryption key from said radio network controller (¶: 131, 135-139);

means for dynamically generating said second encryption key between itself and said radio base station by using said pre-shared key (¶: 131, 135-139); and

means for encrypting the mobile communication traffic by using said second encryption key (¶: 131, 135-139).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 10. A relay node which relays mobile communication traffic between a radio base station and a radio network controller, wherein said relay node is installed in a private network in which said radio base station is installed and relays mobile communication traffic transmitted on said private network between said radio network controller and said radio base station, and said relay node is connected to said radio base station and radio network controller and performs encrypted communication with said radio network controller by using a first encryption key and with said radio base station by using a second encryption key, said relay node comprising:

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and

secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

means for receiving said second encryption key from said radio network controller (¶: 131, 135-139); and

means for encrypting the mobile communication traffic by using said second encryption key (¶: 126).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 11. A radio network controller connected to a plurality of radio base stations via a relay node which performs encrypted communication with said radio base stations by using different encryption keys, said radio network controller comprising: However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items

providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

means for dynamically generating a pre-shared key needed to generate said encryption key between itself and said radio base station by using a key exchange mechanism (¶: 131, 135-139); and

means for notifying said relay node of the generated pre-shared key (¶: 126).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 12. A radio network controller connected to a plurality of radio base stations via a relay node which performs encrypted communication with said radio base stations by using different encryption keys, said radio network controller comprising:

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

means for dynamically generating said encryption key between itself and said radio base stations by using a key exchange mechanism (¶: 131, 135-139); and

means for notifying said relay node of the generated encryption key (¶: 126).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 14. A relay node program allowing a computer serving as a relay node which relays mobile communication traffic between a radio base station and radio network controller to execute a function of relaying mobile communication traffic

transmitted on a private network between said radio network controller and radio base station, and to perform encrypted communication with said radio network controller by using a first encryption key and with said radio base station by using a second encryption key, said computer serving as a relay node and radio base station being installed within said private network, said program further allowing the computer to execute functions of:

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

receiving a pre-shared key for generating said second encryption key from said radio network controller (¶: 135-139, Forslow teaches updating between connections of managing elements and mobile terminal and nodes or gateways take place to authenticate and authorized for session as the sessions keys are verified to take place between the private network and mobile device through nodes);

dynamically generating said second encryption key between itself and said radio base station by using said pre-shared key (¶: 135-139, Forslow teaches updating between connections of managing elements and mobile terminal and nodes or gateways take

place to authenticate and authorized for session as the sessions keys are verified to take place between the private network and mobile device through nodes); and encrypting the mobile communication traffic by using said second encryption key (¶: 135-139, Forslow teaches updating between connections of managing elements and mobile terminal and nodes or gateways take place to authenticate and authorized for session as the sessions keys are verified to take place between the private network and mobile device through nodes).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 15. A relay node program allowing a computer serving as a relay node which relays mobile communication traffic between a radio base station and radio network controller to execute a function of relaying mobile communication traffic transmitted on a private network between said radio network controller and radio base station, and to perform encrypted communication with said radio network controller by using a first encryption key and with said radio base station by using a second

encryption key, said computer serving as a relay node and radio base station being installed within said private network, said program further allowing the computer to execute functions of:

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135-139; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

receiving said second encryption key from said radio network controller (¶: 131, 135-139); and

encrypting the mobile communication traffic by using said second encryption key (¶: 131, 135-139).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of

securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 16. A radio network controller program allowing a computer serving as a radio network controller connected to a plurality of radio base stations via a relay node which performs encrypted communication with said radio base stations by using different encryption keys to execute functions of:

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

dynamically generating a pre-shared key needed to generate said encryption key between itself and said radio base station by using a key exchange mechanism(¶: 126, 131, 135-139); and notifying said relay node of the generated pre-shared key (¶: 131, 135-139).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private

network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 17. A radio network controller program allowing a computer serving as a radio network controller connected to a plurality of radio base stations via a relay node which performs encrypted communication with said radio base stations by using different encryption keys to execute functions of:

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

dynamically generating said encryption key between itself and said radio base station by using a key exchange mechanism (¶: 126, 131, 135-139); and

notifying said relay node of the generated encryption key (¶: 126, 131, 135-139).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented

security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 19. A mobile communication method (abstract, fig. 9) for use in a mobile communication system which comprises:

a radio network controller and a radio base station connected to said radio network controller and which provides a mobile communication service to a mobile terminal connectable to said radio base station, wherein said radio base station and relay node are installed within a private network comprised in said mobile communication system (fig. 9, ¶: 5-9, 46, Watanabe et al. teaches RAN, radio access network, which is a collective term for the radio base station and radio network controller, the RNC controls functionalities for one or more base stations. A base station and a RNC can be the same device, although common set-ups have a separate RNC located in a central office serving multiple base station, despite the fact that they don't have to be physically separated.),

a relay node relays mobile communication traffic transmitted on said private network between said radio network controller and radio base station (fig. 9, ¶: 10, Watanabe et al. teaches VPN, virtual private network, as a relay node installed in said private network which in turn communicates traffic between RAN, radio access networks, and mobile terminal or devices.),

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

first and second encryption keys are used, respectively, between said radio network controller and relay node and between said radio base station and relay node to perform encrypted communication (¶: 135-139, Forslow teaches interactions between mobile client and service manager and correspondent node or gateway to a mobile station and setting security protocols between each connections to assure privacy and content protection between private network and mobile terminal through infrastructure elements), and

a pre-shared key needed to generate said second encryption key is generated by a key exchange mechanism between said radio network controller and radio base station, the generated pre-shared key being notified from said radio network controller to said relay node (¶: 135-139, Forslow teaches updating between connections of managing elements and mobile terminal and nodes or gateways take place to authenticate and authorized for session as the sessions keys are verified to take place between the private network and mobile device through nodes).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Regarding claim 20. A mobile communication method for use in a mobile communication system which comprises:

a radio network controller and a radio base station connected to said radio network controller and which provides a mobile communication service to a mobile terminal connectable to said radio base station, wherein said radio base station is installed within a private network and is connected to a relay node via said private network in said mobile communication system (fig. 9, ¶: 5-9, 46, Watanabe et al. teaches RAN, radio access network, which is a collective term for the radio base station and radio network controller, the RNC controls functionalities for one or more base stations. A base station and a RNC can be the same device, although common set-ups have a separate RNC located in a central office serving multiple base station, despite the fact that they don't have to be physically separated.),

mobile communication traffic between said relay node and radio base station is transmitted on said private network (fig. 9, ¶: 10, Watanabe et al. teaches VPN, virtual private network, as a relay node installed in said private network which in turn communicates traffic between RAN, radio access networks, and mobile terminal or devices and vice versa.),

said relay node relays the mobile communication traffic transmitted on said private network between said radio network controller and radio base station (fig. 9, ¶: 10, Watanabe et al. teaches VPN, virtual private network, as a relay node installed in said private network which in turn communicates traffic between RAN, radio access networks, and mobile terminal or devices.),

However, Watanabe et al. was not found to discloses the specific limitations described below, nevertheless, Forslow teaches encryption methods used between network items providing through these means a mobile client secure data access to the VPN and secure data access to the mobile client (¶: 66-67, 93, 107-109, 131, 135; Forslow teaches security keys and other method for encrypting or securing information from attacks and keeping information transmissions through the private network and other devices private).

first and second encryption keys are used, respectively, between said radio network controller and relay node and between said radio base station and relay node to perform encrypted communication (¶: 135-139, Forslow teaches interactions between mobile client and service manager and correspondent node or gateway to a mobile station and setting security protocols between each connections to assure privacy and

content protection between private network and mobile terminal through infrastructure elements), and

said second encryption key is dynamically generated by a key exchange mechanism between said radio network controller and radio base station, the generated second encryption key being notified from said radio network controller to said relay node (¶: 135-139, Forslow teaches updating between connections of managing elements and mobile terminal and nodes or gateways take place to authenticate and authorized for session as the sessions keys are verified to take place between the private network and mobile device through nodes).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention of Watanabe et al. to specifically include the security protocols used by Forslow between mobile terminal and nodes and network elements as so taught in Forslow, for the purposes of ensuring components that constitute and unprecedented security lock, effectively isolating a distributed workgroup into a mobile virtual private network (abstract). One skilled in the art would be motivated since the two inventions that of Forslow and Watanabe et al. are dealing with similar objectives and obstacles of securing the private network by using a VPN through implementation of network elements that communicate with private source or corporation.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DIEGO HERRERA whose telephone number is (571)272-0907. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester Kincaid can be reached on (571) 272-7922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Diego Herrera/
Examiner, Art Unit 2617

/Lester Kincaid/

Supervisory Patent Examiner, Art Unit 2617